



DPC: 24/30481276 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 July 2024

Origin: International

Latest date for receipt of comments: 01 September 2024

Project No. 2023/02357

Responsible committee: AUE/16 Data Communication (Road Vehicles)

Interested committees:

Title: Draft BS ISO 13400-2 Road vehicles - Diagnostic communication over Internet Protocol (DoIP). Part 2: Transport protocol and network layer services.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 01 September 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 13400-2

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2: Transport protocol and network layer services

*Véhicules routiers — Communication de diagnostic au travers du
protocole internet (DoIP) —*

Partie 2: Protocole de transport et services de la couche réseau

ICS: 43.040.10; 43.180

ISO/TC 22/SC 31

Secretariat: **DIN**

Voting begins on:
2024-07-09

Voting terminates on:
2024-10-01

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/DIS 13400-2:2024(en)

Full document details: 24/30481276 DC

© ISO 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Symbols and abbreviated terms	4
4.1 Symbols	4
4.2 Abbreviated terms	4
5 Conformance	6
6 DoIP introduction	6
6.1 General information	6
6.2 Connection establishment and vehicle discovery	7
6.2.1 Direct connection scenario	7
6.2.2 Network connection scenario	8
6.2.3 Internal tester scenario (optional)	8
6.2.4 Unsecured DoIP session	8
6.2.5 Secured (TLS) DoIP session	10
6.3 Vehicle network integration	11
6.3.1 Vehicle identification	11
6.3.2 Multiple vehicles in a single network	12
6.4 Communication examples using message sequence charts	13
6.5 IP-based vehicle communication protocol — General information	14
7 Application (APP)	14
7.1 APP - Implementation of DoIP requirements	14
7.2 APP - Data transmission order	14
7.3 APP - DoIP entity synchronization of a vehicle's GID	14
7.4 APP - Vehicle identification and announcement request message	17
7.5 APP - Diagnostic power mode information request and response	23
7.6 APP - DoIP entity status information request and response	23
7.7 APP - Timing and communication parameters	24
7.8 APP - Logical address assignment	25
7.9 APP - Communication environments and recommended timings	26
7.10 APP - DoIP entity functional requirements	26
8 Service interface	27
8.1 General	27
8.2 Abstrat service primitive (ASP) parameters	28
8.2.1 ASP - Data type definitions	28
8.2.2 ASP - DoIP_AI, address information	28
8.2.3 ASP - Length, length of PDU	29
8.2.4 ASP - PDU, protocol data unit	29
8.2.5 ASP - DoIP_Result	29
8.3 ASP - DoIP layer service interface	30
8.3.1 ASP - DoIP_Data.request	30
8.3.2 ASP - DoIP_Data.indication	30
8.3.3 ASP - DoIP_Data.confirm	30
9 Application layer (AL)	31
9.1 AL – Dynamic host control protocol (DHCP)	31
9.1.1 AL – General	31
9.1.2 AL – IP address assignment	32
9.1.3 AL – IP address validity and renewal	35
9.2 AL – Generic DoIP protocol message structure	36

9.3	AL – Handling of UDP packets and TCP data	41
9.4	AL – Supported payload types over TCP and UDP ports	41
9.5	AL – Diagnostic message and diagnostic message acknowledgement	42
9.6	AL – Alive check request and alive check response	47
9.7	AL – Periodic response message structure	48
9.8	AL – DoIP transport protocol payload type status message structure	50
10	Transport layer security (TLS)	54
10.1	TLS – Secure diagnostic communication	54
10.2	TLS – DoIP security profile	57
10.2.1	TLS – General	57
10.2.2	TLS – Accepted TLS versions for DoIP	57
10.2.3	TLS – Accepted cipher suites	57
10.2.4	TLS – Accepted TLS extensions	58
11	Transport layer (TL)	59
11.1	TL – Transmission control protocol (TCP)	59
11.2	TL – User datagram protocol (UDP)	61
11.3	TL – Handling of UDP messages	65
12	Network layer (NL)	65
12.1	NL – Internet protocol (IP)	65
12.2	NL – IPv4 address resolution protocol (ARP)	65
12.3	NL – IPv6 neighbour discovery protocol (NDP)	66
12.4	NL – Internet control message protocol (ICMP)	66
12.5	NL – IP-based vehicle communication protocol	66
12.6	NL – Socket handling	72
12.6.1	NL – Connection states	72
12.6.2	NL – General inactivity timer	75
12.6.3	NL – Initial inactivity timer	75
12.6.4	NL – Socket handler and alive check	76
13	Data link layer (DLL)	79
13.1	DLL – General	79
13.2	DLL – MAC-layer	79
	Bibliography	80

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

This third edition cancels and replaces the second edition (ISO 13400-2:2019), which has been technically revised.

The main changes compared to the previous edition are as follows:

- implemented ISO 13400-2:2019/Amd 1:2023(E) with corrections;
- modified Figure 1 to show ISO 13400-2 DoIP payload type detection;
- specified the DoIP protocol version = 4 for this edition;
- updated [subclause 7.7](#) APP - Timing and communication parameters, [Table 12](#);
- added new requirement 7.DoIP-190 AL – DoIP entity diagnostic message NACK code set to 09₁₆;
- added new requirement 7.DoIP-191 AL – DoIP transport protocol payload type status and message structure;
- added new requirement 7.DoIP-192 AL – DoIP entity checks for supported payload types over UDP Ports;
- modified [Figure 16](#) to include 7.DoIP-192 new requirement.

A list of all parts in the ISO 13400 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Vehicle diagnostic communication has been developed starting with the introduction of the first legislated emissions-related diagnostics and has evolved over the years, now covering various use cases ranging from emission-related diagnostics to vehicle-manufacturer-specific applications like calibration or electronic component software updates.

With the introduction of new in-vehicle network communication technologies, the interface between the vehicle's servers and the client DoIP entity has been adapted several times to address the specific characteristics of each new network communication technology requiring optimized data link layer definitions and transport protocol developments in order to make the new in-vehicle networks usable for diagnostic communication.

With increasing memory size of servers, the demand to update this increasing amount of software and an increasing number of functions provided by these control units, technology of the connecting network and buses has been driven to a level of complexity and speed similar to computer networks. Various applications (x-by-wire, infotainment) require high band-width and real-time networks (like FlexRay, MOST), which cannot be adapted to provide the direct interface to a vehicle. This requires gateways to route and convert messages between the in-vehicle networks and the vehicle interface to client DoIP entity.

All parts of ISO 13400 are applicable to vehicle diagnostic systems implemented on an IP communication network.

The ISO 13400 series has been established in order to define common requirements for vehicle diagnostic systems implemented on an IP communication link.

Although primarily intended for diagnostic systems, ISO 13400 has been developed to also meet requirements from other IP-based systems needing a transport protocol and network layer services.

The intent of the ISO 13400 series is to describe a standardized vehicle interface which

- separates in-vehicle network technology from the client DoIP entity vehicle interface requirements to allow for a long-term stable external vehicle communication interface,
- utilizes existing industry standards to define a long-term stable state-of-the-art communication standard usable for legislated diagnostic communication as well as for manufacturer-specific use cases,
- can easily be adapted to new physical and data link layers, including wired and wireless connections, by using existing adaptation layers, and
- allows connections of vehicle-internal and vehicle-external DoIP entities.

To achieve this, it is based on the Open Systems Interconnection (OSI) Basic Reference Model specified in ISO/IEC 7498-1 and ISO/IEC 10731,^[1] which structures communication systems into seven layers.

[Figure 1](#) illustrates an overview of communication frameworks beyond the scope of this document including related standards:

- Vehicle diagnostic communication framework, which is composed of ISO 14229-1,^[3] ISO 13400-2 (DoIP payload type detection), ISO 14229-2,^[4] and ISO 14229-5^[5].
- Presentation layer standards, for example vehicle manufacturer- (VM-) specific or ISO 22901 ODX^[7].
- OSI lower layers framework, which is composed of ISO 13400-3 and ISO 13400-4^[2].

The ISO 13400 series and ISO 14229-5^[5] are based on the conventions specified in the OSI Service Conventions (ISO/IEC 10731)^[1] as they apply for all layers and the diagnostic services.

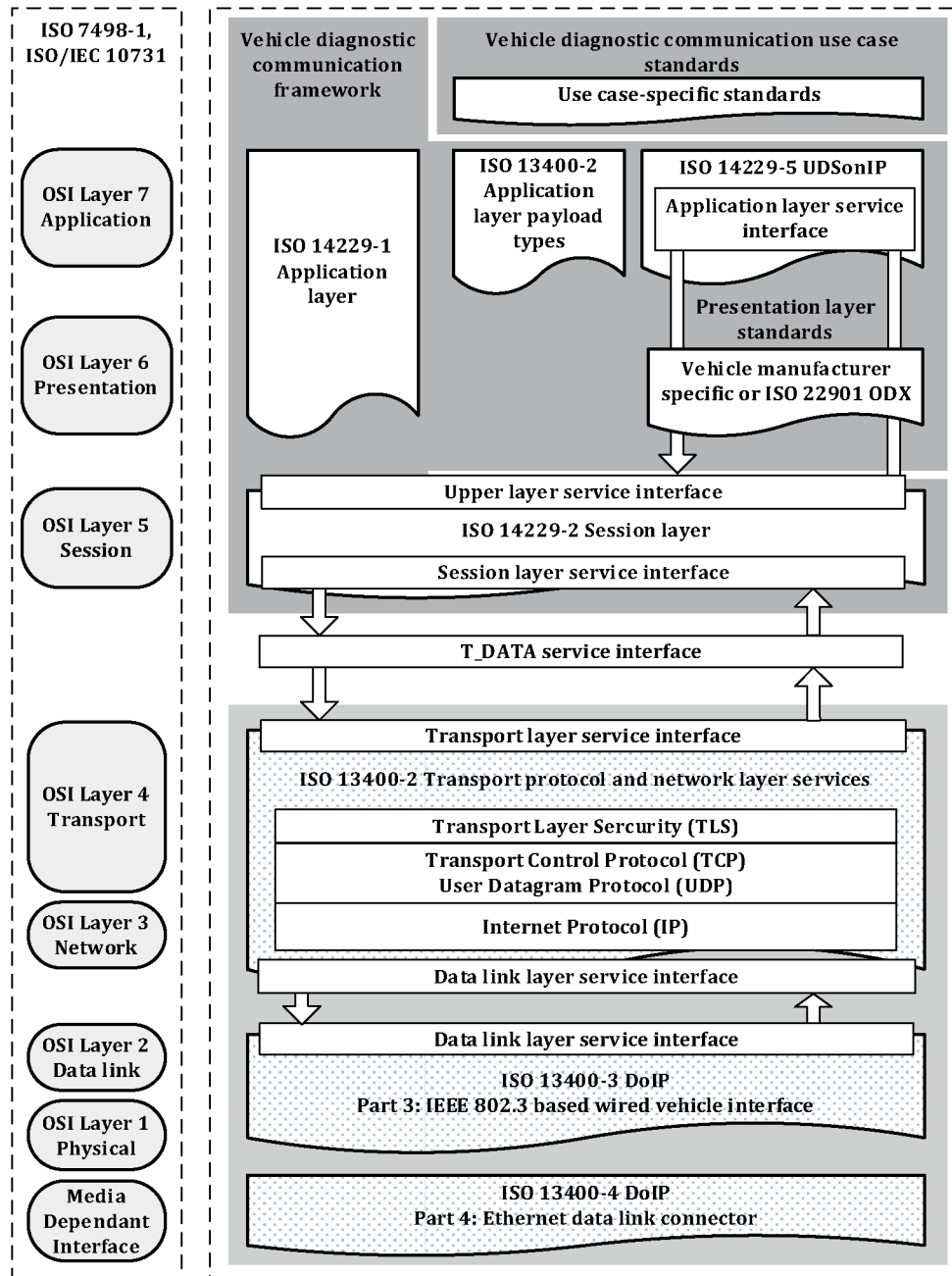


Figure 1 — DoIP document reference according to OSI model

Figure 2 illustrates vehicle network architecture schematics from a functional viewpoint.

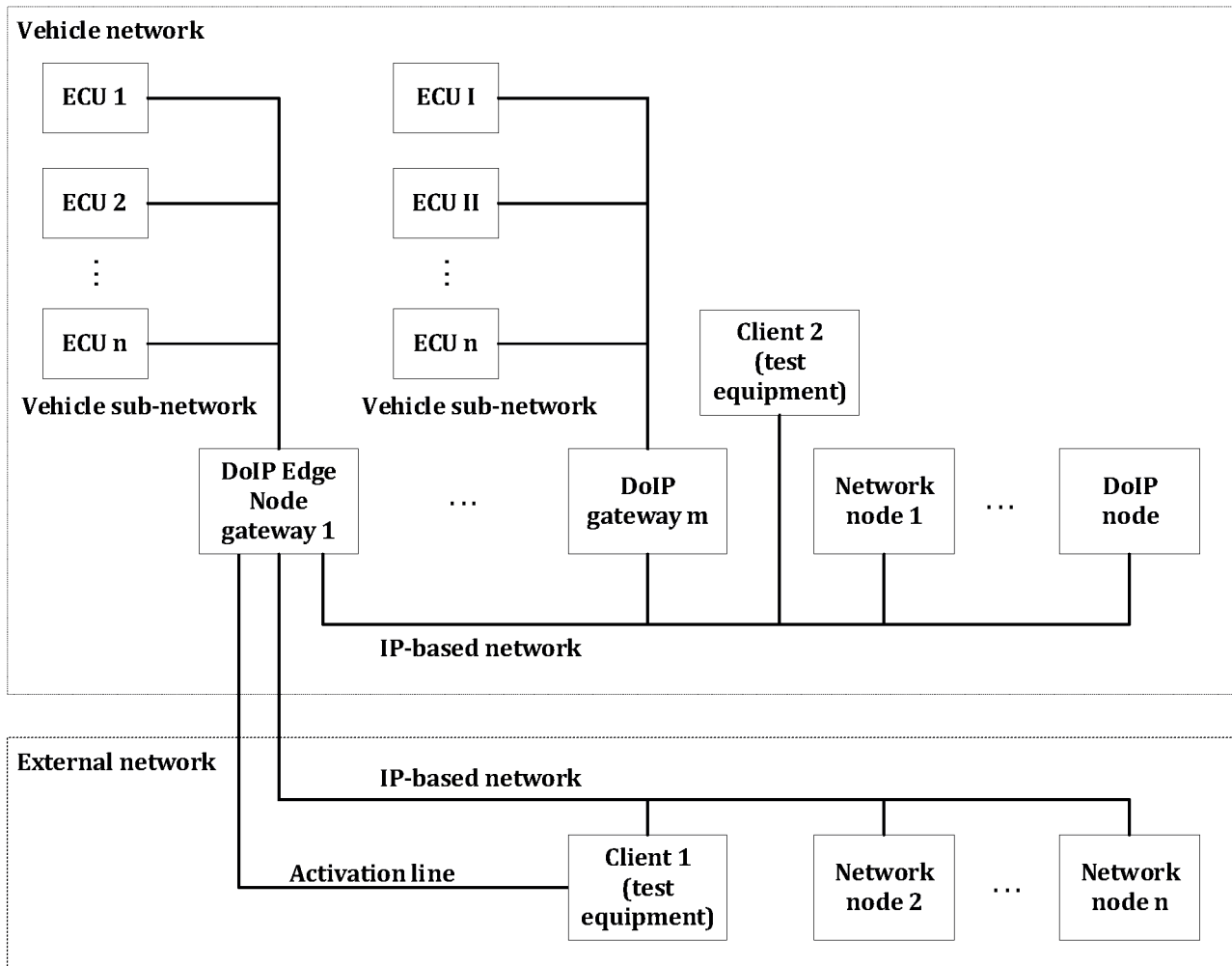


Figure 2 — Vehicle network architecture schematics (functional view)

This protocol standard is implemented by one or more DoIP entities, depending on the vehicle's network architecture. [Figure 2](#) illustrates a client 1 (external client), which is connected to the DoIP edge node and a client 2 (internal client) in the vehicle's internal network. If not stated otherwise, the DoIP client entities are assumed to behave the same regardless to which network they are connected.

If necessary, this document distinguishes between an “internal client” and “external client” to apply a requirement or statement.

In this document, the requirements are assigned a unique number of the form “X.DoIP-yyy”, allowing for easier requirement tracking and reference.

- X = OSI layer number; and
- DoIP-yyy = requirement number; and
- xL = x = OSI layer abbreviation [8 = APP, 7 = AL, 6 = PL, 5 = SL, 4 = TL, 3 = NL, 2 = DLL, 1 = PHY, 0 = ASP].

NOTE Requirements in this document are not numbered sequentially because the order of individual requirements changed during document development.

Requirements formulated as “The vehicle shall implement ...” imply that this is a requirement for all DoIP entities to implement the required functionality if not explicitly stated otherwise. If multiple DoIP entities are present on a vehicle network, implementation details may differ slightly for each DoIP entity (e.g., for identification purposes), so that the client DoIP entity is able to identify the individual DoIP gateways that support this protocol standard.

Where reference is made to RFC documents, note that the forms “shall/shall not” are used to express requirements in these documents.

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2: Transport protocol and network layer services

1 Scope

This document specifies the requirements for secured and unsecured diagnostic communication between client DoIP entity and server(s) installed in the vehicle using Internet protocol (IP) as well as the transmission control protocol (TCP) and user datagram protocol (UDP). This includes the definition of vehicle gateway requirements (e.g., for integration into an existing computer network) and test equipment (client DoIP entity) requirements (e.g., to detect and establish communication with a vehicle).

This document specifies features that are used to detect a vehicle in a network and enable communication with the vehicle gateway as well as with its sub-components during the various vehicle states. These features are separated into two types: mandatory and optional.

This document specifies the following mandatory features:

- vehicle network integration (IP address assignment);
- vehicle announcement and vehicle discovery;
- vehicle basic status information retrieval (e.g., diagnostic power mode);
- connection establishment (e.g., concurrent communication attempts), connection maintenance and vehicle gateway control;
- data routing to and from the vehicle's sub-components;
- error handling (e.g., physical network disconnects).

This document specifies the following optional features:

- DoIP entity status monitoring;
- transport layer security (TLS);
- DoIP entity firewall capabilities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 13400-3, *Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 3: Wired vehicle interface based on IEEE 802.3*

ISO/IEC/IEEE 8802-3, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 3: Standard for Ethernet*

IETF RFC 768, *User Datagram Protocol*

IETF RFC 791:1981, *Internet Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 792, *Internet Control Message Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 793, *Transmission Control Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 826, *An Ethernet Address Resolution Protocol*

IETF RFC 1122, *Requirements for Internet Hosts — Communication Layers*

IETF RFC 2131, *Dynamic Host Configuration Protocol*

IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) — Specification*

IETF RFC 2375, *IPv6 Multicast Address Assignments*

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

IETF RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local Addresses*

IETF RFC 4291, *IP Version 6 Addressing Architecture*

IETF RFC 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol Version 6 (IPv6) Specification*

IETF RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

IETF RFC 8446:2018, *The Transport Layer Security (TLS) Protocol Version 1.3*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

diagnostic power mode

abstract vehicle internal power supply state, which affects the diagnostic capabilities of all servers on the in-vehicle networks and which identifies the state of all servers of all gateway sub-networks that allow diagnostic communication

Note 1 to entry: The intent is to provide information to the client DoIP entity about whether diagnostics can be performed on the connected vehicle or whether the vehicle needs to be put into a different diagnostic power mode (i.e. technician interaction required). In this document, the following states are relevant: Not Ready (not all servers accessible via DoIP can communicate), Ready (all servers accessible via DoIP can communicate) and Not Supported (the Diagnostic Information Power Mode Information Request message is not supported).

3.2

DoIP edge node

host (3.4) inside the vehicle, where an Ethernet activation line in accordance with ISO 13400-3 is terminated and where the link from the first node/host in the external network is terminated

[SOURCE: ISO 13400-3:2011, 3.1.2, modified — definition editorially revised.]

3.3

DoIP entity certificate

certificate issued by an *intermediate CA* (3.5) to the DoIP entity presented during the TLS handshake to the client DoIP entity to verify the authenticity of this DoIP entity

3.4

host

node connected to the IP-based network

3.5

intermediate certificate authority

intermediate CA

authority, which issues subordinal certificates to another intermediate CA or DoIP entities

3.6

intermediate certificate

certificate either stored in the client DoIP entity or is presented during authentication together with the end node certificate to complete the chain of trust

3.7

invalid source address

address outside the reserved range for client(s) DoIP entity

3.8

logical address

address identifying a diagnostic application layer entity

3.9

network node

device connected to the IP-based network (e.g., Ethernet) and which communicates using Internet protocol but does not implement the DoIP protocol

Note 1 to entry: Some network nodes might also be connected to a *vehicle sub-network* (3.14), but they are not DoIP gateways as they don't implement the DoIP protocol. Consequently, these network nodes do not interact with (e.g., respond to) DoIP-compliant client DoIP entity.

3.10

root certificate authority

authority, which acts as the root of trust

Note 1 to entry: Typically issues *intermediate certificates* (3.6) to allow an *intermediate CA* (3.5) to further submit certificates.

3.11**root certificate**

certificate created by the *root certificate authority* (3.10) and used as the trust anchor

Note 1 to entry: It is securely stored and used by all entities that wants to validate end node certificates (e.g., from the DoIP entity) together with all necessary *intermediate certificates* (3.6) in the chain of trust.

3.12**socket**

unique identification, as defined in IETF RFC 147,^[12] to or from which information is transmitted in the network

3.13**unknown source address**

address not listed in the connection table entry

3.14**vehicle sub-network**

network not directly connected to the IP-based network

Note 1 to entry: Data can only be sent to and from a vehicle sub-network through the connecting DoIP gateway.

4 Symbols and abbreviated terms**4.1 Symbols**

<d>	payload length, given in bytes
<m>	number of concurrent DoIP TCP sessions that the client DoIP entity is required to support in order to connect to one or more DoIP entities
<n>	number of concurrent DoIP TCP sessions that the DoIP entity needs to support in order to accept 1 to N concurrent connections to one or more items of the client DoIP entity
<u>, <v>	number of individual servers in a vehicle sub-network
<w>	number of individual DoIP gateways in a vehicle network
<x>	number of individual in-vehicle network nodes
<y>	number of individual vehicle DoIP nodes in a vehicle network
<z>	number of individual vehicle external network nodes

4.2 Abbreviated terms

AL	application layer
Alt	alternative
APP	application
ARP	address resolution protocol
ASCII	American standard code for information interchange
Auto-MDI(X)	automatic medium-dependent interface crossover
C	condition

CA	certificate authority
CAN	controller area network
CF	consecutive frame
Cvt	convention: mandatory, optional
DHCP	dynamic host control protocol
DLL	data link layer
DNS	domain name system
DoIP	diagnostic communication over Internet Protocol
EID	entity identification
FC	flow control
FF	first frame
FMI	failure mode indicator
GID	group identification
GUI	graphical user interface
GW	gateway
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
IETF RFC	Internet Engineering Task Force Request for Comments
IP	Internet protocol
IPv4	Internet protocol version 4 (see IETF RFC 791)
IPv6	Internet protocol version 6 (see IETF RFC 2460)
M	mandatory
MAC	media access control
MCTS	maximum concurrent <code>TCP_DATA</code> sockets
MDS	maximum data size
MSC	message sequence chart
MTU	maximum transport unit
NCTS	currently open <code>TCP_DATA</code> sockets
NDP	neighbour discovery protocol
NL	network layer
NT	node type

O	optional
OSI	open systems interconnection
PKI	public key Infrastructure
RX	reception
SA	source address
SDU	service data unit
SF	single frame
SOM	start of message
SPN	suspect parameter number
ASP	abstract service primitive
TA	target address
TCP	transmission control protocol
TL	transport layer
TLS	transport layer security
TX	transmission
UDP	user datagram protocol
VIN	vehicle identification number (see ISO 3779 ^[14])
VM	vehicle manufacturer
XOR	exclusive or

5 Conformance

This document is based on the conventions discussed in the OSI Service Conventions as specified in ISO/IEC 10731^[1] as they apply to diagnostic services.

6 DoIP introduction

6.1 General information

This subclause gives an example of a standard workflow of a straightforward DoIP session. In order to keep this introduction as helpful as possible for a reader new to DoIP, exceptions and errors that might occur during a DoIP session are not covered here. Two possible network environments—networked and directly connected—are explained. The figures provide a better understanding of the comprised DoIP components, mechanisms and sequences that allow a proper DoIP session.

As only the connection and the vehicle discovery (see 7.4) differ between the direct connection and the networked scenarios, the homogeneous parts of the DoIP session are described in [Figure 11](#) for both scenarios.

6.2 Connection establishment and vehicle discovery

6.2.1 Direct connection scenario

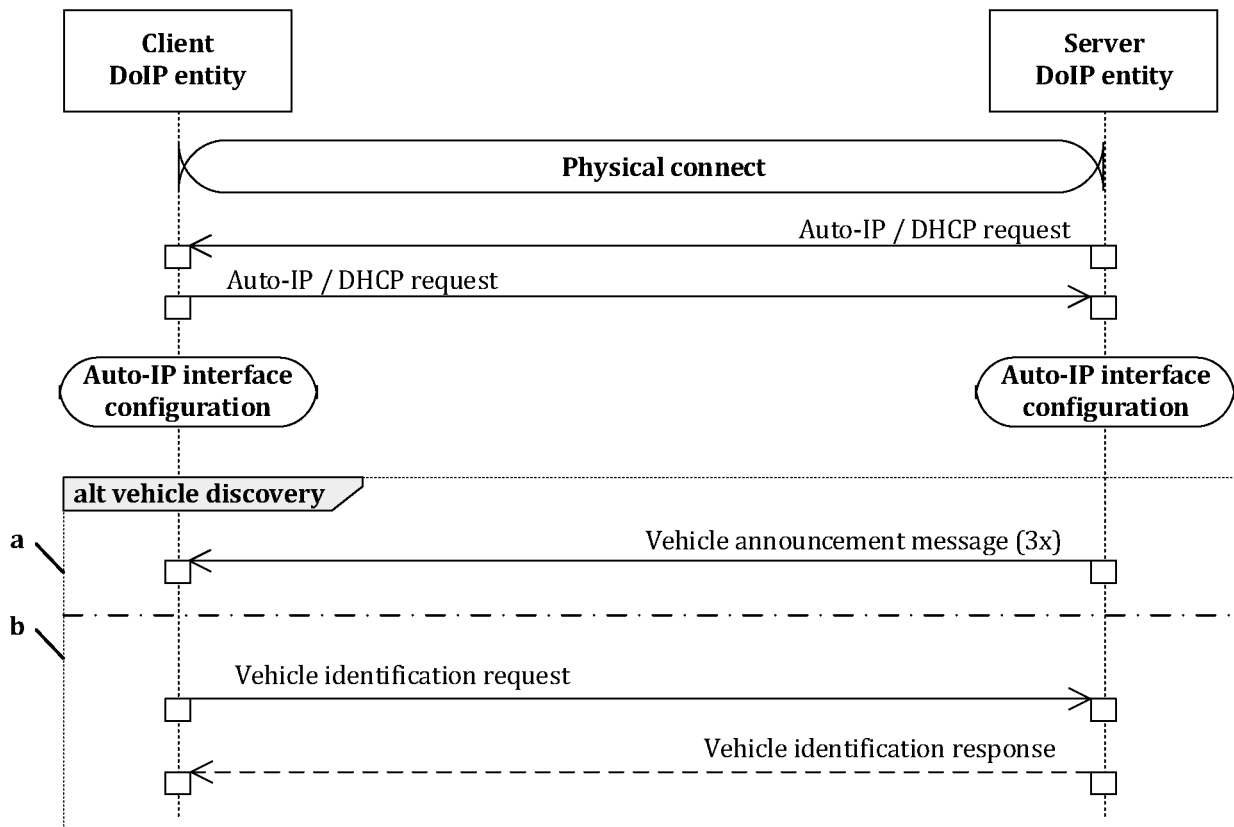
In a direct connection scenario with no networking infrastructure, a “crossover” Ethernet cable is used or Auto-MDI(X) is supported by the Ethernet controller by either the client DoIP entity or the DoIP entity (server), in order to directly connect the vehicle to the client DoIP entity.

It is assumed that, in such a scenario, no DHCP server is present. Thus, although initiated, the DHCP process is not successful. Rather, a locally valid IP address is determined by the auto-configuration mechanism and afterwards configured for both interfaces involved.

As soon as the DoIP entity's interface is configured with the obtained IP address, the DoIP entity broadcasts its vehicle identification number (VIN), entity identification (EID), group identification (GID), and logical address through a vehicle announcement message (see 7.4). The message is broadcasted (UDP) three times with the destination port UDP_DISCOVERY.

Depending on whether the client DoIP entity is configured in time for TCP/IP communication to receive the initial vehicle announcement messages, the client DoIP entity may poll for a vehicle using the vehicle identification request message. The Auto-IP mechanism might be delayed on the client DoIP entity as some operating systems start the Auto-IP only after DHCP has failed. As the DoIP entity initiates both mechanisms in parallel, it is likely that its IP configuration is completed quickly and the client DoIP entity does not receive the initial vehicle announcement.

Figure 3 shows the connection and vehicle discovery in a direct connection scenario.



Key

- a client is already reachable
- b client did not receive the initial vehicle announcement

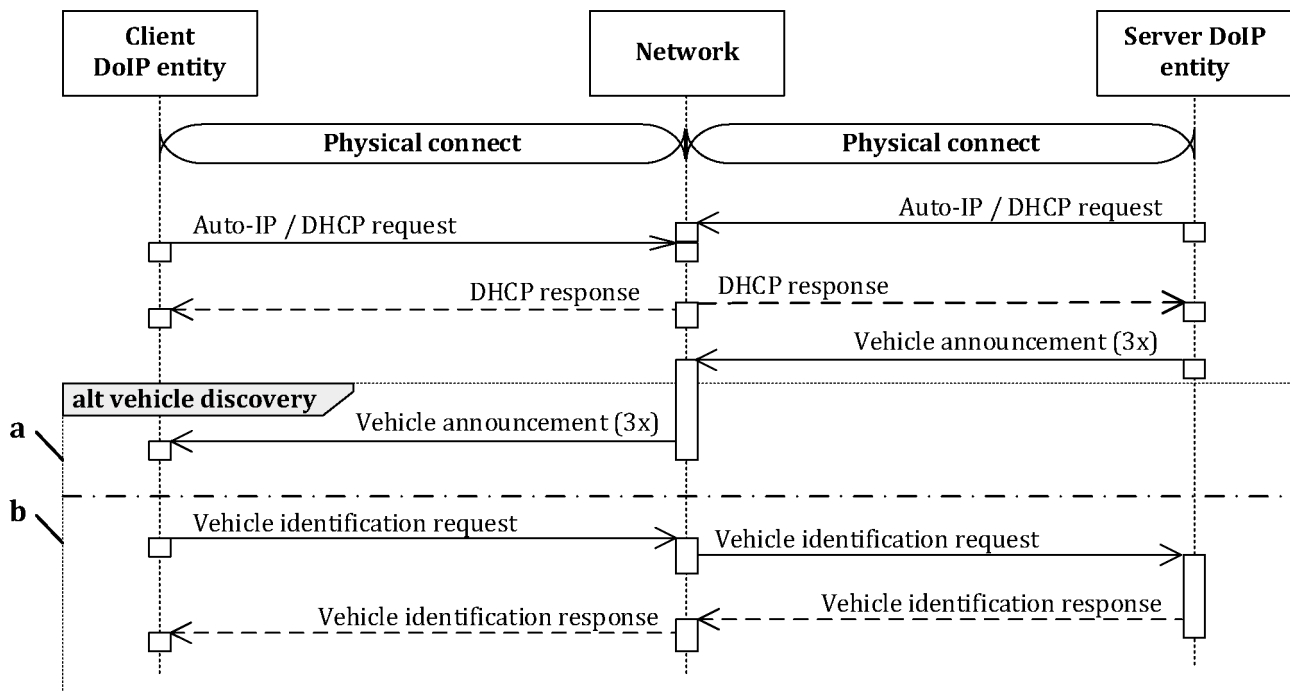
Figure 3 — Connection and vehicle discovery in a direct connection scenario

6.2.2 Network connection scenario

The connection and vehicle discovery process are slightly different in a networked scenario. The physical connections to the network are not necessarily synchronized in time. Accordingly, the points in time when the interfaces are configured and accessible for a TCP/IP connection attempt might differ significantly.

In certain network scenarios, there can be multiple vehicles sending vehicle announcement messages. If the vehicle's DoIP entity does not send a vehicle announcement message, the client DoIP entity can poll for the vehicle announcement message by sending vehicle identification request messages.

Figure 4 depicts the connection and vehicle discovery in a networked scenario.



Key

- a client is already reachable
- b client did not receive the initial vehicle announcement

Figure 4 — Connection and vehicle discovery in a networked scenario

6.2.3 Internal tester scenario (optional)

Use cases like "Over-The-Air" OTA software update or remote diagnostics use vehicle internal test equipment. Internal test equipment can omit dynamic IP address assignment via DHCP or AutoIP to enable minimal interface startup times by using static IP address configuration. This also applies to vehicle announcements on vehicle-internal IP interfaces.

6.2.4 Unsecured DoIP session

The step "add vehicle to list" (see Figure 5) is not covered by this document and thus it is not mandatory or may not even be necessary. Nevertheless, it is likely, that the vehicle announcement message broadcast in the previous step is processed in some way. For example, the vehicle somehow indicates to be "ready" or an automated process is initiated based on the information that a vehicle is now available for a DoIP session.

Although in the networked scenario there is still the networking equipment between the client and the DoIP entity, the communication is now logically directly between the two communication endpoints. Thus, no network is shown in Figure 5.

The first step in order to initiate a connection between the client DoIP entity and the DoIP entity in the vehicle is to open a socket (destination port is `TCP_DATA`). This is done prior to any message exchange. Therefore, a DoIP entity provides the resources to handle the incoming communication request (e.g., socket resources). The DoIP entity provides sufficient resources to handle the specified number of concurrently supported DoIP sessions ($\langle n \rangle$) plus one extra socket (see DoIP-002). If more than $\langle n + 1 \rangle$ connection attempts arrive at the same time, it is possible that no more resources are free and the $\langle n + 2 \text{nd} \rangle$ connection attempt is refused (because there are no longer any sockets in the listening state because of DoIP protocol handling).

Once a socket is established, some initializing steps are performed. An initial inactivity timer (see [12.6.3](#)) and a general inactivity timer (see [12.6.2](#)) is assigned and started. Additionally, it is necessary to ensure that no arriving data, except the routing activation request message, is routed or processed by setting the connection state to “initialize” (see [12.6.1.3](#)). All subsequent messages are exchanged through this `TCP_DATA` socket. This connection handling is also applied by the DoIP entity in case of secure TLS-based communication and the corresponding `TCP_DATA` TLS socket (see [6.2.5](#)).

To activate routing on the initialized connection, the client sends a routing activation request message (see [12.5](#)) to the DoIP entity. If the client DoIP entity is eligible and if there are fewer than $\langle n \rangle$ active connections registered, the corresponding initial timer is stopped and—assuming that no additional authentication or confirmation or secure TLS connection is required—the socket state changes to “registered [routing active]”. Now valid DoIP messages (e.g., DoIP diagnostic messages) are routed or processed. This is reported to the client DoIP entity by a positive routing activation response message. The general inactivity timer is restarted and remains active.

When receiving any kind of data, the DoIP entity first calls the DoIP header handler. If the payload consists of a diagnostic message (identified through the payload type `800116` in the generic DoIP header, see [9.5](#)), the diagnostic message handler is called to process the payload.

When a diagnostic message arrives, the DoIP confirmation is sent to the calling client DoIP entity immediately after the message has successfully passed the diagnostic message handler (confirmation acknowledgement), in essence the message has passed through the corresponding internal routing mechanism but has not yet been processed by the DoIP gateway or forwarded to the final non DoIP server.

In the case of an ISO 14229-1^[3] conform diagnostic message payload, the destination server DoIP entity sends a diagnostic response back to the client DoIP entity. This behaviour is described by the corresponding diagnostic protocol encapsulated by the DoIP message and thus is not within the scope of this document.

When a connection is no longer required by the client DoIP entity, it always closes through TCP/IP protocol mechanisms. The DoIP entity then initiates a finalization process for the connection. That finalization frees the corresponding resources so that the socket is available for a new connection. If the connection is not closed, the resources are freed after a timeout based on the general inactivity timer or after the performance of an alive check.

[Figure 5](#) depicts the unsecured DoIP session example.

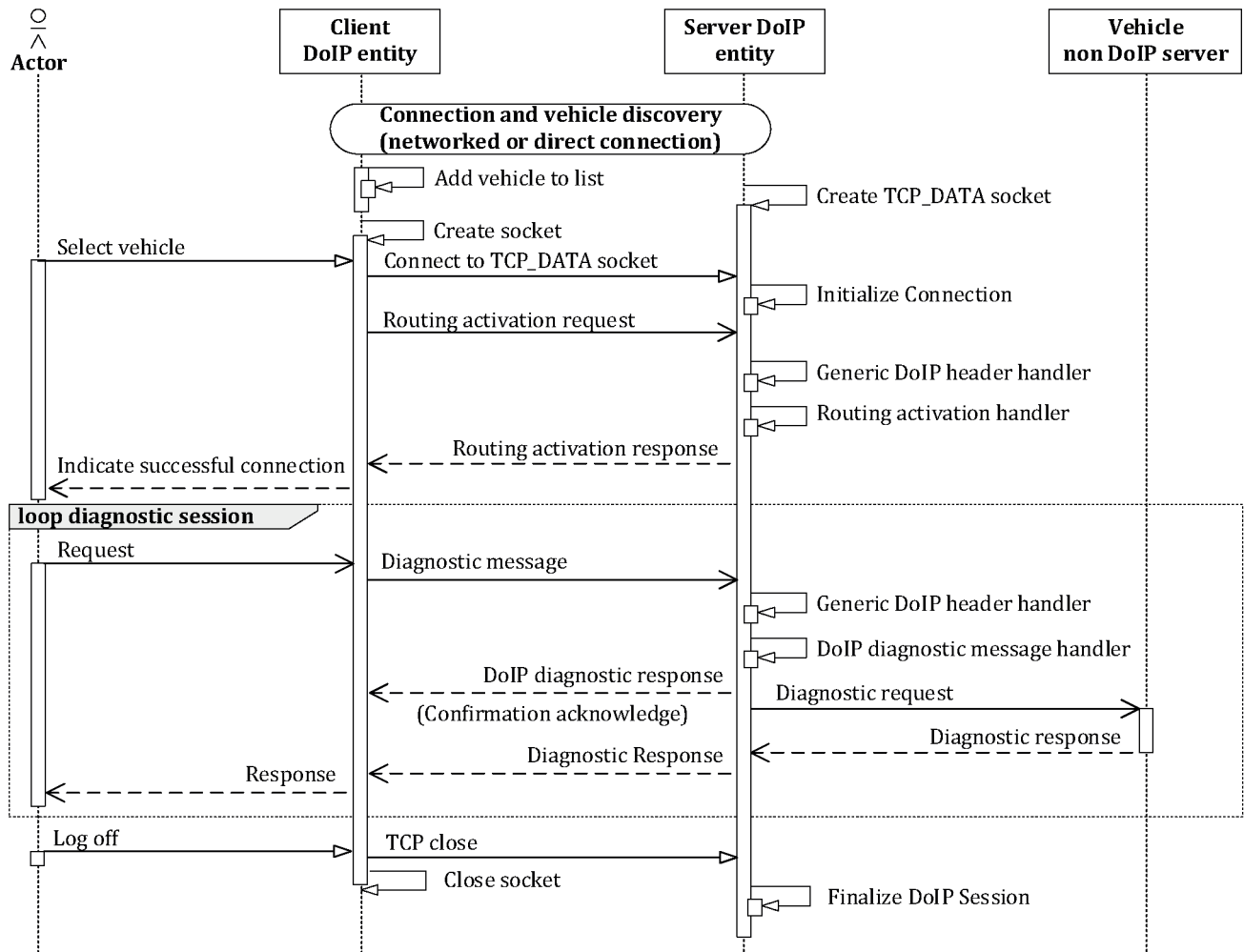


Figure 5 — Unsecured DoIP session example

6.2.5 Secured (TLS) DoIP session

For a secured TCP connection, the TLS dedicated TCP_DATA port is used. As for the unsecured DoIP session case, the first step in order to initiate a secure TLS connection between the client DoIP entity and the DoIP entity, is to open a TLS socket (destination port is TLS TCP_DATA). This is done prior to any message exchange. Therefore, a DoIP entity provides the resources to handle the incoming communication request (e.g. socket resources). The DoIP entity provides sufficient resources to handle the specified number of concurrently supported DoIP sessions secured with TLS (<k>) (see [DoIP-159]). If more than <k> connection attempts do arrive at the same time, it is possible that no more resources are available and the <k + 1st> connection attempt is refused (because there are no longer any sockets in the listening state because of DoIP protocol handling).

A vehicle manufacturer may choose to implement k+1 TLS data sockets, where the additional socket is used to reject a routing activation with routing activation response code 01₁₆.

If a k+1 TLS data socket is not implemented, no DoIP routing activation response code 01₁₆ can be responded when all k concurrently supported DoIP sessions are already in use. In this case, the additional connection will be rejected on the TCP level already.

[Figure 6](#) shows the DoIP session secured with TLS example.

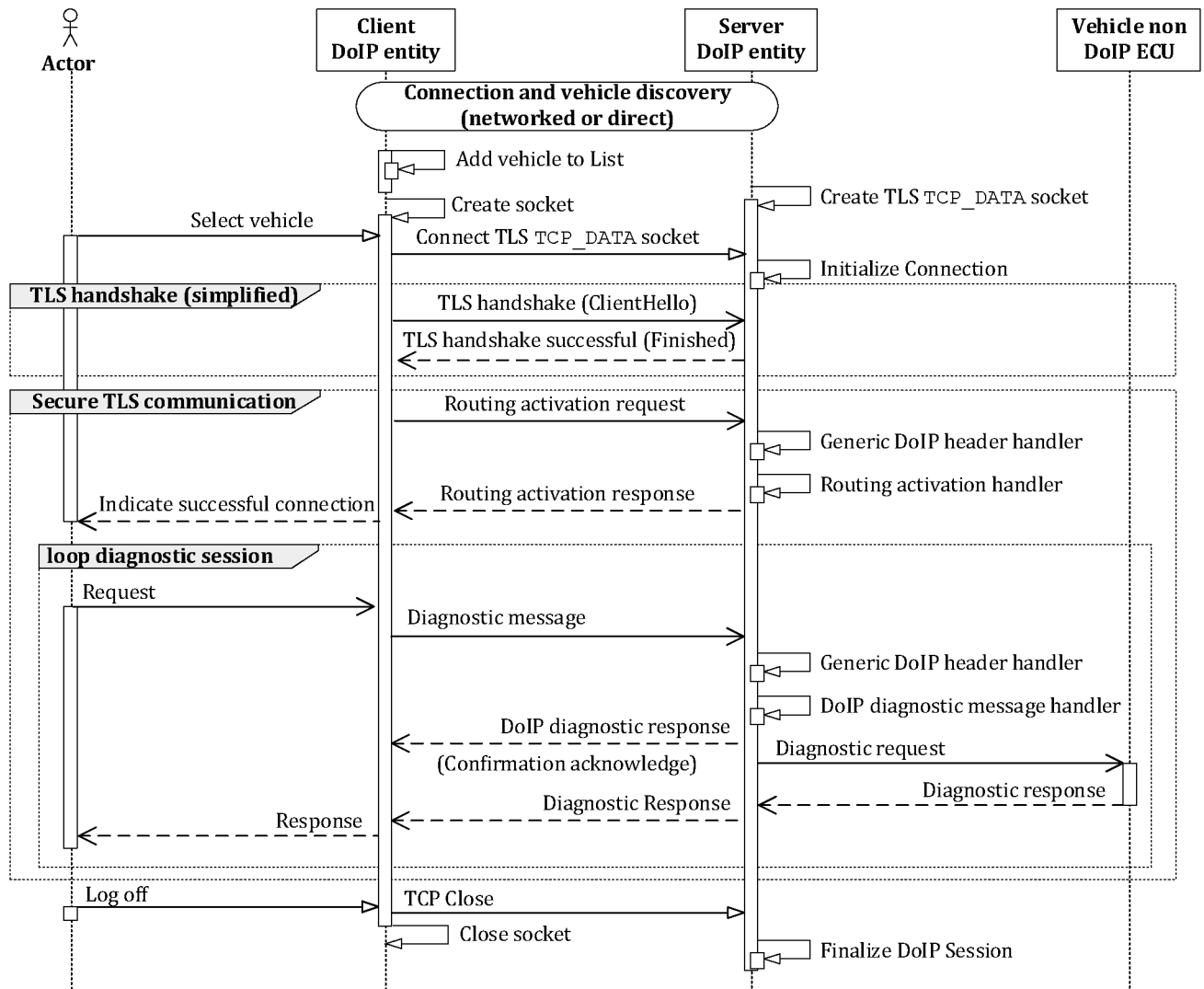


Figure 6 — Secured DoIP session with TLS example

When the secured TCP connection is no longer required by the client DoIP entity, it always closes cleanly through TLS and TCP/IP protocol mechanisms (see e.g., TLS 1.2 RFC 5246:2008, 7.2.1, TLS 1.3 RFC 8446:2018, 6.1). The DoIP entity also destroys any TLS related information of the current session and make available the corresponding resources so that the TLS socket is available for a new connection.

6.3 Vehicle network integration

6.3.1 Vehicle identification

Vehicle identification specifies how a vehicle and its DoIP entities can be discovered and associated with their IP addresses on the network.

A vehicle is usually identified by its VIN. In manufacturing or in after-sales environments, several DoIP entities may be installed on the same vehicle, but the vehicle-specific VIN is not yet configured at this point in time. In order to associate newly installed and un-configured DoIP entities with a vehicle, the group ID (GID) can be used instead of the VIN.

6.3.2 Multiple vehicles in a single network

This subclause gives an example of a sequence by which the external client DoIP entity may be able to identify and group server DoIP entities of all connected vehicles within a network.

[Figure 7](#) shows an example of a simplified identification sequence performed by the client DoIP entity. When a vehicle is connected to the DoIP network and the IP address allocation is completed (see [Figure 5](#)), the DoIP entities send out vehicle announcements after waiting for A_DoIP_Announce_Wait.

If the client DoIP entity is connected to the DoIP network at a later time, it should trigger vehicle announcement/identification responses by sending a broadcast vehicle identification request.

The server DoIP entities in all vehicles respond to a vehicle identification request within A_DoIP_Ctrl.

If a vehicle announcement/vehicle identification is received by the client DoIP entity and contains a VIN/GID synchronization status incomplete message (10_{16}), meaning that the VIN or GID is *not* synchronized with all server DoIP entities in the vehicle, the client DoIP entity starts a vehicle discovery timer for this vehicle (identified by the VIN/GID given by the VIN/GID master in its vehicle announcement/vehicle identification response).

This mechanism allows the VIN/GID master to notify the client DoIP entity when some entities need more time for VIN/GID synchronization. When the vehicle discovery timer expires, another vehicle identification request is sent to all those DoIP entities, which reported VIN/GID invalid in their initial vehicle announcement/identification responses.

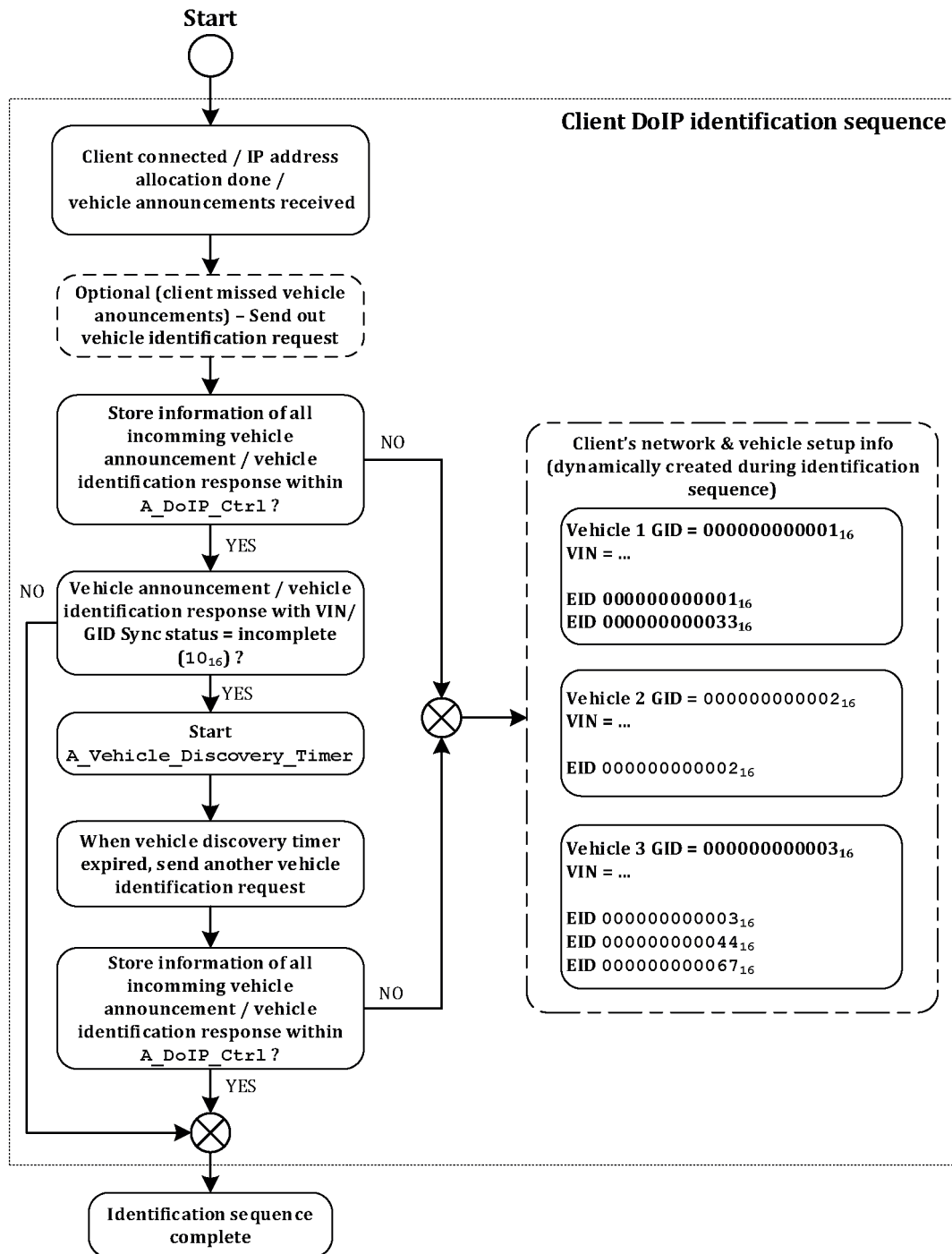


Figure 7 — Example of a simplified identification sequence of client

6.4 Communication examples using message sequence charts

Several message sequence charts (MSCs) show the most common communication scenarios of client DoIP entity communication with server DoIP entities of a vehicle.

6.5 IP-based vehicle communication protocol — General information

The tables in [7.4](#) to [7.6](#), [9.2](#) to [9.6](#), and [12.5](#) describe each message under the following column headings:

- Item:
This is a short name for the message element. This name is used when the message element is referenced in this document.
- Pos.:
This is the position (byte number) of each individual message element in a DoIP message. The byte position always starts with zero (0) and is counted from the beginning of the PDU.
- Len:
This is the length (number of bytes) of the respective message element.
- Description:
This column contains a more detailed description of each individual message element and its purpose.
- Values:
This column lists the supported value range and meaning of individual values of the respective message element.
- Support:
This column contains information on whether a specific message or message element is supported by a DoIP entity. Even if a message itself is defined as optional, it may contain mandatory elements to be implemented if the message itself is supported.
- Port and protocol:
This column specifies on which underlying protocol a specific payload type is supported and which port it uses.

7 Application (APP)

7.1 APP - Implementation of DoIP requirements

REQ	8.DoIP-108 APP - This document's implementation
Each DoIP entity on a vehicle network shall implement the protocol requirements as specified in this document.	

7.2 APP - Data transmission order

REQ	8.DoIP-147 APP - Big-endian network byte order
The big-endian network byte order of IP shall be used for DoIP messages in accordance with IETF RFC 791:1981, Annex B.	

7.3 APP - DoIP entity synchronization of a vehicle's GID

A group identification (GID) is a decentralized approach for identifying multiple DoIP entities within one vehicle. This implies that there is a VIN/GID master (e.g., the DoIP edge node) from which all other DoIP entities receive the VIN/GID during a synchronization process. As this synchronization process usually requires some time (e.g., after a new DoIP entity is added to the vehicle) invalidity values are defined (see [Table 1](#)) for use by the DoIP entities until the VIN/GID synchronization is finished.

A detailed specification of VIN/GID synchronization between DoIP entities is outside the scope of this document and is left to the VM's discretion.

REQ	8.DoIP-143 APP – DoIP entity synchronization of a vehicle's GID
Each DoIP entity shall support the synchronization of a vehicle's GID if more than one DoIP entity is present within the vehicle and if the availability of a valid VIN cannot always be guaranteed to be configured for every DoIP entity.	

NOTE One possible way to ensure a globally unique GID is to use the GID masters MAC address.

Figure 8 describes schematically the VIN/GID synchronization and identification of two separate DoIP entities within the same vehicle.

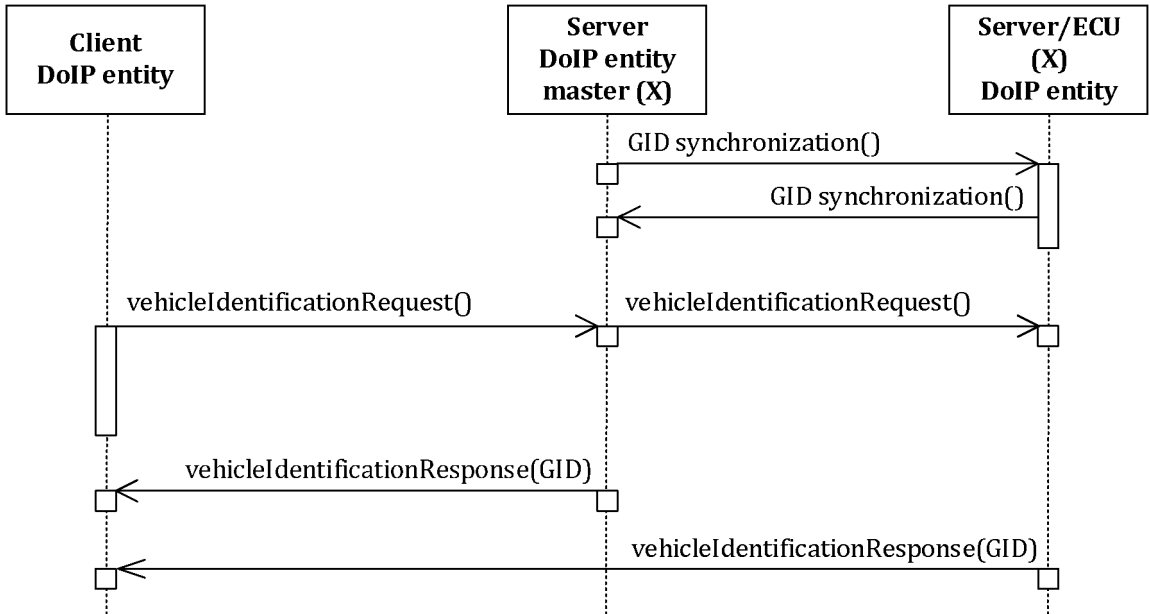


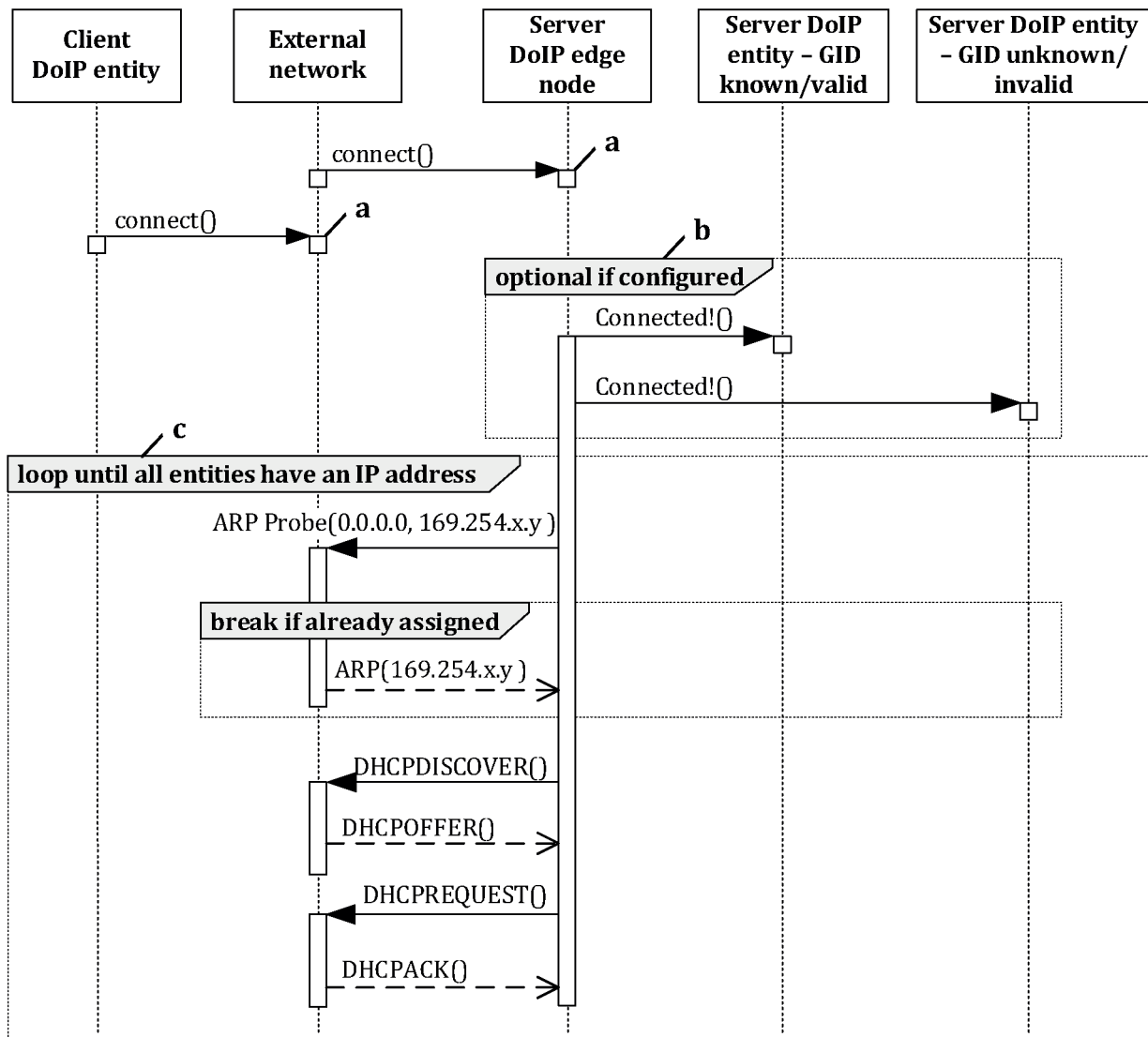
Figure 8 — Example of vehicle identification with VIN/GID synchronization

Table 1 specifies the values if parameter value is not set.

Table 1 — Vehicle identification parameter values (value not set)

Parameter	Length	Values
VIN	17	00 ₁₆ or FF ₁₆
Logical address	2	0000 ₁₆ or FFFF ₁₆
Entity ID (EID)	6	00 ₁₆ or FF ₁₆
Group ID (GID)	6	00 ₁₆ or FF ₁₆

Figure 9 shows the sequence for connecting client DoIP entity to the vehicle and the IP address allocation process.



Key

- a This will activate the activation line and supply a physical data link connection.
- b How this information is conveyed is not specified in this document.
- c This might happen for all nodes concurrently. Only one node is shown for simplicity.

Figure 9 — Detailed vehicle identification without VIN/GID synchronisation

[Figure 10](#) describes in more detail the complete decentralized approach of identifying multiple DoIP entities.